Protecting Credit/Debit Card Information

1. Credit/debit card payment information should be kept secured and confidential at all times.
   1. Credit/debit card information should be secured in a locked area (room or closet).
   2. The area designated to store credit/debit card information should be restricted to the department designee responsible for processing or researching a transaction.
   3. Any credit/debit card point of sale terminal should be placed in a secure area to prevent access to data within the terminal.
   4. If the secured location is within an office, where other employees have access, it is recommended to store the information in a locked file cabinet or desk.
   5. Access to credit/debit card data should be restricted to those individuals whose job requires such access. A privileged user list should be maintained by the department.
2. All but the last four digits of the account number should be marked through (masked) when displaying a cardholder data receipt that includes the merchant and customer copy and any other form that may contain credit/debit card information.
3. Pin pads or any magnetic strip readers should not be attached to a credit/debit card terminal or computer. Credit/debit card information may not be stored in any device used for credit/debit card processing.
   1. Security data/track is defined as the data elements stored within the magnetic stripe on the back of a card, as well as the cardholder validation code (the three or four digit value printed on the signature panel of the card).
   2. The information includes all the data required to commit fraud on a cardholder’s account.
   3. The only data a merchant may store is the cardholder’s name, account number, expiration data and authorization code. Once authorization has been received the data must be deleted.
4. Credit/debit card payment information cannot be stored on computers or networks, regardless of encryption. In addition, credit card information cannot be sent via end-user messaging technologies (text messaging).
5. Credit/debit card information must be transmitted and received in a secure manner.
   1. If your department received credit/debit card payment information by fax and/or mail, all digits of the card number except the last four, must be marked through before retaining for your records.
   2. Credit/debit card information should not be sent to a fax application with an IP address.
   3. Fax machines should be in secured area (room with a locking door) with no through traffic and with limited access.
   4. Credit/debit information should not be received by email.
6. Credit/debit card receipts should be stored according to WKU’s record retention schedule. All receipts must be shredded after that time.
7. All devices should be periodically inspected to look for tampering or substitution. If you suspect suspicious behavior, or tampering has occurred, contact the Bursar’s Office immediately.
8. Additional Policy information can be found at: <http://www.wku.edu/policies/docs/143.pdf>